

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the matter of the search of
an Apple iPod, Model A1421, bearing serial number
CCQPK392FMJF (the "subject electronic device"), further depicted
in Attachment A.

Case No. 4:23 MJ 8179 SRW

SIGNED AND SUBMITTED TO THE COURT FOR FILING
BY RELIABLE ELECTRONIC MEANS

FILED UNDER SEAL**APPLICATION FOR A SEARCH WARRANT**

I, Eric Lanham, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

21 U.S.C. §§ 841(a) & 846
 18 U.S.C. §§ 924(c) & 924(j)

Offense Description

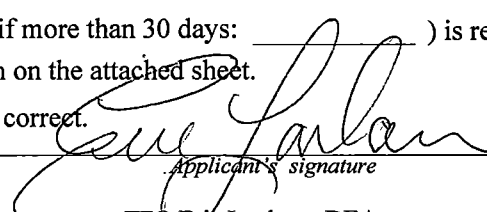
Conspiracy to possess with intent to distribute a controlled substance
 Possession of a firearm in furtherance of a drug trafficking crime resulting in death

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.


 Applicant's signature

TFO Eric Lanham, DEA
 Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal
 Procedure 4.1 and 41.

Date: 06/21/2023

City and state: St. Louis, MO


 Judge's signature
 Honorable Stephen R. Welby, U.S. Magistrate Judge
 Printed name and title

AUSA: REA

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF an)
Apple iPod, Model A1421, bearing serial) No. 4:23 MJ 8179 SRW
number CCQPK392FMJF (the “**subject**) *Signed and Submitted to the Court for*
electronic device”), further depicted in) *filing by reliable electronic means*
Attachment A.) **FILED UNDER SEAL**
)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Eric Lanham, a Detective with the City of Bridgeton Missouri Police Department, and currently assigned to the Drug Enforcement Administration, being duly sworn states:

I. APPLYING OFFICER/BACKGROUND INFORMATION

1. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

2. I have been a deputized Task Force Officer with the Drug Enforcement Administration (DEA) since 2004 and am currently assigned to an Enforcement Group of the St. Louis Division Office. My parent law enforcement agency is the City of Bridgeton where I have been employed as a sworn police officer for the last 29 years.

3. During my tenure with DEA and as a Task Force Officer, I have been assigned to an investigative team for numerous complex investigations of drug-trafficking organizations dealing in heroin, cocaine, marijuana, and other controlled substances. These investigations have resulted in the seizure of heroin, fentanyl, methamphetamine, marijuana, other controlled substances, and weapons. I am familiar with and have utilized normal methods of investigation,

including, but not limited to, visual surveillance, questioning of witnesses, the use of search and arrest warrants, the use of informants, the use of pen registers, the utilization of confidential sources and the use of court-authorized wire intercepts. My training with the Drug Enforcement Administration and as a sworn police officer has included specific training directly related to the aforementioned investigative techniques.

4. Currently, I am part of a team of experienced law enforcement officers/agents who are investigating the criminal activities, specifically the narcotics distribution and associated murder and violence, committed by Anthony JORDAN a/k/a “TT,” a/k/a “Godfather,” and others. JORDAN has prior arrests for Murder 1st Degree; Armed Criminal Action; Felonious Restraint; Trafficking in Drugs 2nd Degree; Resisting Arrest; and Unlawful Use of Weapon. In 2005, JORDAN received a Suspended Imposition of Sentence for Unlawful Use of Weapon.

II. INTRODUCTION

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. This affidavit is submitted in support of an application for the issuance of a search warrant for the following described cellular telephone:

- a. An Apple iPod, Model A1421, bearing serial number CCQPK392FMJF (the “**subject electronic device**”). The electronic device is depicted in Attachment A, which is incorporated herein by this reference (photographs attached).

7. The instant application is a request for the acquisition of data stored in the above-described **subject electronic device** seized pursuant to the execution of a federal search warrant

on August 7, 2015.

8. Presently, the **subject electronic device** is in the custody of the United States Attorney's Office located at 111 South 10th Street, St. Louis, Missouri 63102, within the Eastern District of Missouri.

9. As further detailed below, investigators previously obtained authority to search and seized the **subject electronic device** pursuant to a Search and Seizure Warrant issued by the Honorable Judge Noelle C. Collins, United States Magistrate Judge for the Eastern District of Missouri on October 6, 2015 (4:15 MJ 3238 NCC). On or about October 7, 2015, an examiner with the Federal Bureau of Investigation (FBI) examined the **subject electronic device**. At that time, the examiner was unable to bypass the passcode of the **subject electronic device** and as a result, could not extract data from the **subject electronic device**. Another examination of the **subject electronic device** was undertaken by the FBI on November 3, 2015. Again, the examiner was unable to bypass the passcode of the **subject electronic device** and as a result, could not extract data from the **subject electronic device**.

10. It is my opinion as an experienced, trained narcotics investigator that there exists probable cause to believe that evidence will be found of violations of Title 21, United States Code, Sections 841 and 846 (Possession with Intent to Distribute/Distribution of Controlled Substances and/or Conspiracy to Distribute or Possess with the Intent to Distribute), Title 18 United States Code, Section 924(j) (Discharging a Firearm in furtherance of a Drug Trafficking Crime where death results), and Title 18 United States Code, Section 924(c) (Possession of Firearms in Furtherance of a Drug Trafficking Crime), (collectively the "subject offenses") in the **subject electronic device** (as described in Attachment B). The controlled substances which are the primary focus of this investigation are heroin, a Schedule I controlled substance and cocaine, a

Schedule II controlled substance. In addition, based on information from a confidential source relative to several murders, as outlined below, evidence will further be gathered relative to violations of Title 18, United States Code, Sections 922(g), 924(c) and 924(j).

11. The items to be seized are fruits, instrumentalities, and evidence of violations of the subject offenses, as described in Attachment B, which is incorporated herein by reference.

III. HISTORY AND BACKGROUND

12. Beginning in 2013, investigators identified Anthony JORDAN as a multiple kilogram heroin and cocaine trafficker. An investigation ensued and investigators received information that JORDAN and his co-conspirators, were involved in an on-going feud with a rival drug faction. According to a confidential source hereinafter identified as CS#1, JORDAN committed several murders of the rival drug faction's members and associates.

13. CS #1 has had a long-standing relationship with JORDAN, which included CS #1 being supplied with narcotics by JORDAN, via communication over cellular telephones, as well as CS#1's participation in shootings and murders of the rival drug faction. Discussions in these matters were also facilitated over cellular telephones. CS #1 also indicated that JORDAN utilized the cameras and storage capacities of cellular telephones and other electronic devices to store information related to or memorialize his commission of the subject offenses. CS #1 has testified before a federal Grand Jury relative to these matters and has made statements against his/her own personal interest. CS #1 provided the information which led to the issuance of the federal search warrants as outlined above and the subsequent seizure of the **subject electronic device** of the instant application. The information provided by CS #1 has been found to be accurate in all material respects and further corroborated by the overall seizures made in conjunction with the execution of the federal search warrants.

14. On August 6, 2015, United States Magistrate Judge David D. Noce, seated in the Eastern District of Missouri, authorized three federal search warrants for locations associated with the Anthony JORDAN Drug Trafficking Organization (DTO). One such location was 4223 W. Sacramento, St. Louis, Missouri, in the Eastern District of Missouri. This residence was believed to be owned by a family member of JORDAN, however, was under the direct control of JORDAN. On August 7, 2015, investigators executed the federal search warrant on 4223 W. Sacramento and seized numerous items of evidentiary value including fourteen cellular telephones.

15. On August 26, 2015, a Grand Jury sitting in the Eastern District of Missouri returned an indictment against Anthony JORDAN for violations of Title 21 United States Code, Sections 841 and 846 (conspiracy to distribute cocaine) and Title 18 United States Code, Section 924(j) (Discharging a Firearm in furtherance of a Drug Trafficking Crime where death results (4:15 CR 404 HEA)). A federal arrest warrant was issued.

16. On or about August 27, 2015, JORDAN was arrested at 64 Brighton Park, Saint Charles, Missouri. A 2005 light green Pontiac Grand Prix was located in the driveway and had been identified as a vehicle connected to JORDAN. The vehicle was seized.

17. On September 16, 2015, investigators executed a federal search warrant on the 2005 light green Pontiac Grand Prix. Investigators recovered a T-Mobile white Samsung Galaxy SIII cellular telephone from that vehicle. Investigators later secured a federal search warrant on that Samsung Galaxy phone. A forensic examiner searched that phone and recovered, *inter alia*, screenshots of JORDAN holding a firearm, screenshot of ballistic damage to a vehicle and a news story reporting Anthony “Blinky” Clark’s homicide. Presently, JORDAN is charged with Discharging a Firearm in furtherance of a Drug Trafficking Crime where death results in connection to the murder of Anthony “Blinky” Clark (4:15 CR 404 HEA). Investigators believe

this demonstrates that JORDAN uses cellular telephones and other electronic devices to engage in violations of the subject offenses and maintain information on those devices related to these offenses.

18. The **subject electronic device** was also located inside and seized from the 2005 light green Pontiac Grand Prix. A physical analysis of the **subject electronic device** has determined that the **subject electronic device** is equipped with a camera and possesses storage capabilities for electronic media. In light of, among other things, the **subject electronic device's** seizure from inside the same vehicle where the above-described T-Mobile white Samsung Galaxy SIII cellular telephone was recovered, and the **subject electronic device's** camera and storage capabilities, investigators believe that JORDAN may have also utilized the **subject electronic device** to engage in violations of the subject offenses and maintain information on the **subject electronic device** related to these subject offenses.

19. As indicated above, following the seizure of the **subject electronic device**, on October 6, 2015, the Honorable Judge Noelle C. Collins, United States Magistrate Judge for the Eastern District of Missouri authorized a federal search warrant to search the **subject electronic device** (4:15 MJ 3238 NCC). As described above, On or about October 7, 2015, an examiner with the Federal Bureau of Investigation (FBI) examined the **subject electronic device**. At that time, the examiner was unable to bypass the passcode of the **subject electronic device** and as a result, could not extract data from the **subject electronic device**. Another examination of the **subject electronic device** was undertaken by the FBI on November 3, 2015. Again, the examiner was unable to bypass the passcode of the **subject electronic device** and as a result, could not extract data from the **subject electronic device**. The investigative team did not possess the technology for accessing the **subject electronic device** in October and November 2015.

20. Recently, I have spoken to Saint Louis County Police Department Intelligence Analyst Megan Buffa, who is also assigned to DEA, and understand that with the advancement of technology related to electronic forensics, the **subject electronic device** may now be able to be “unlocked” for data extraction and analysis.

21. Based on all of the above information, your affiant asserts that there is probable cause to believe that evidence related to the subject offenses will be located on the **subject electronic device**.

22. The **subject electronic device** is currently secured at the United States Attorney’s Office, St. Louis, Missouri. Based upon conversations with investigators and in my training and experience, I understand that the **subject electronic device** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state, as it was when it first came into the possession of the FBI and later the United States Attorney’s Office. Accordingly, all evidence present on the **subject electronic device** at the time of its seizure on August 7, 2015 will still be there and available to examiners.

IV. DEFINITIONS AND TERMINOLOGY CELLULAR AND MOBILE TELEPHONES

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).
- b. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example,

tablets, digital music devices, portable electronic game systems, electronic game consoles and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- c. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- d. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- e. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- f. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.
- g. "Wireless telephone or mobile telephone, or cellular telephone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the

telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- h. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- i. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store any digital data, such as word processing documents, even if the device is not designed to access such files. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- j. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- k. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

V. TRAINING AND EXPERIENCE OF THE INVESTIGATIVE TEAM

24. During my career as a law enforcement officer, I have conducted numerous drug investigations including those of urban poly drug trafficking organizations. Based on my training and experience in such investigations, including Title III interceptions, electronic surveillance investigations, I and other members of the investigative team, know that drug traffickers communicate with each other utilizing cellular telephones and other electronic devices to facilitate the overall scheme of their illicit endeavors. In order to be successful, drug traffickers must communicate via telephones and other electronic devices to orchestrate the importation of controlled substances; to manage and maintain contact with drug couriers; to maintain contact with lower level distributors in their day-to-day operations; to maintain contact with safe house operators where narcotics are stored; and to coordinate the return movement of the drug derived profits back to the sources of supply.

25. Further based on my experience and training, I am cognizant that drug traffickers oftentimes "dump" or exchange their telephones and other electronic devices for new instruments. Further insulating themselves from law enforcement detection, drug traffickers are known to subscribe to electronic service in other persons names and to frequently change their telephone number, ESN's/IMSI numbers, screen names, and attempt to mask internet protocol addresses.

26. I also know from prior Title III investigations and subsequent de-briefing of involved parties by investigative team members, that drug traffickers are known to compartmentalize the use of multiple telephones and other electronic devices. As an example, a subject will use a certain telephone and other electronic devices to contact sources of supply,

another telephone and other electronic devices to contact couriers, other telephones and other electronic devices to contact underlings, so forth and so on. De-briefing of co-conspirators and captured court authorized wire interceptions have revealed that the above methods are employed to thwart law enforcement's ability to detect members of a drug trafficking organization and conduct electronic surveillance on co-conspirators. Based on the sheer number of cellular telephones and other electronic devices seized from the outlined residence, investigators believe that JORDAN and members of his Drug Trafficking Organization (DTO) are compartmentalizing the use of their telephones and other electronic devices, as related above.

27. With my experience and training, and that of other task force officers and special agents, as well as detectives on the investigating team, and participation in investigations involving the distribution of controlled substances, from speaking with other agents and officers, and our investigation further detailed in this affidavit, we have also learned the following:

- a. Drug trafficking is traditionally a cash intensive enterprise due to its illicit nature, the desire to avoid records of sales, and the complexities of introducing this cash into the financial system. Persons involved in drug trafficking will often hold large amounts of cash on hand in their businesses and residences.
- b. Persons involved in drug trafficking rely heavily on mobile telephones and other electronic devices to conduct activities related to and in furtherance of the criminal activity. Mobile telephones and other electronic devices are used to pass communications, such as instructions, negotiations, directions, and locations, both verbally and in writing via electronic message.

- c. Narcotics traffickers tend to associate with others involved in illegal activity, and frequently use mobile telephones and other electronic devices, GPS units, and other wireless communication devices in furtherance of their crimes to communicate with co-conspirators. I also know that drug traffickers often carry multiple phones or devices to facilitate their communications, sometimes using different devices (or groups of devices) to communicate with different parts of their drug trafficking network (e.g. customers, transporters, suppliers, etc.) Narcotics traffickers and distributors also switch out multiple cellular phones and other electronic devices in order to avoid detection by law enforcement. Pre-paid phones are typically used in this fashion, as they are harder to track since they require less verifiable information about the phone's subscriber.
- d. In order to make it easier for drug currency and narcotics traffickers to communicate with one another, their phones and other devices often contain stored telephone numbers, programmed names, addresses, and encrypted codes and names. I also know that the phones and other communication devices of currency and narcotics traffickers often contain voicemails, text messages, photographs and emails relating to communications with co-conspirators, meeting locations as well as the telephone numbers of co-conspirators who have called or been called by the device.
- e. Persons involved in the distribution of controlled substances will

disguise the distribution through a business operation and maintain business records, including but not limited to records and financial statements. I also know from my experience and training, as well as from discussions I have had with other law enforcement officers, that such records and documents are kept and stored in computers and electronic-memory devices in addition to or in lieu of hard-copy versions of this data. Similar to filing cabinets, boxes, or other physical devices for such records and documents, computers, electronic storage media and peripherals are commonplace and are often located inside residences. Further, documents and records can be "hidden" within such electronic storage media.

- f. Persons who possess, purchase, or sell firearms generally maintain the firearms and records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as a residence. Many people also keep mementos of their firearms, including digital photographs or videotapes of themselves possessing or using firearms on their cell phones/smart phones, computers, flash drives and portable hard drives. It has been my experience that prohibited individuals who purchase firearms illegally may keep the contact information of the individual who is supplying firearms to the criminal element for future purchases or referrals. Many people do not dispose of their firearms-related records; they usually keep their records for long periods, often

spanning several years, in a secure location within their residence. As noted above, many of the seized telephones contained photographs of firearms and/or text messages (with contact information) that appear to be related to the utilization of firearms.

28. Based on my training, experience, and research, I know that devices such as the **subject electronic device** to be searched have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, along with evidence of the subject offenses.

29. There is probable cause to believe that things that were once stored on the **subject electronic device** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual

memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

30. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the subject offenses described on the warrant, but also forensic evidence that establishes how the media to be searched was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the media to be searched because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not

present on a storage medium.

31. Devices such as the **subject electronic device** now offer a broad range of capabilities. These capabilities may include, but are not limited to: taking, sending, receiving, and storing still photographs and moving video; and accessing and downloading information from the Internet. These devices may also include global positioning system (“GPS”) technology for determining the location of the device.

VI. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND MOBILE COMPUTING SYSTEMS

32. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he/she often stores it in random order and with deceptive file names. The latter requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Moreover, the vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. As such, it is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

33. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (NOTE: The following is a non-exclusive list, as other search procedures may be employed):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as listed in Attachment B;
- b. Searching for and attempting to recover any deleted, hidden, and/or encrypted data to determine whether that data falls within the list of items to be seized as listed in Attachment B (any data that is encrypted and/or unreadable will be returned when law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. Surveying various file directories and the individual files they contain;
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

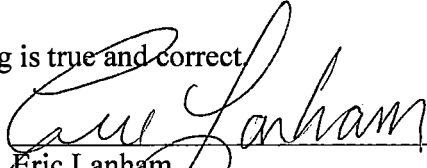
VIII. CONCLUSION

34. In view of the foregoing, there is probable cause to conclude that, in the digital media to be searched within the **subject electronic device**, there will be located evidence of a crime, contraband, the fruit or instrumentalities of a crime, of one or more violations of Title 21, United States Code, Section 841(a) and 846 (unlawful manufacture, distribution, or possession with intent to distribute a controlled substance and conspiracy), as well as evidence relative to violations of Title 18, United States Code, Sections 924(c) and 924(j). Because this investigation

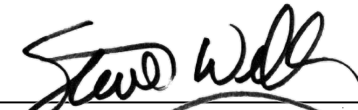
is ongoing and its success would be jeopardized if the contents of this affidavit were made public at this time, I am requesting that this affidavit and the accompanying search warrant documents be sealed until ordered unsealed by the Court.

35. Accordingly, I respectfully request the issuance of a warrant to search the **subject electronic device** listed in Attachment A for the items described in Attachment B.

I state under penalty of perjury the forgoing is true and correct.


Eric Lanham
Task Force Officer
Drug Enforcement Administration

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 21st day of June 2023.


HONORABLE STEPHEN R. WELBY
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

Subject electronic device: An Apple iPod, Model A1421, bearing serial number CCQPK392FMJF (the “**subject electronic device**”). The electronic device is depicted in Attachment A, which is incorporated herein by this reference (photographs attached).

This warrant authorizes the forensic examination of the above device, including any micro SD, SIM cards, memory cards or other storage media attached to or inside the devices to be searched which are used as extended memory storage devices, for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT "B"
(LIST OF INFORMATION TO BE
SEIZED)

1. All records on the **subject electronic device** including the evidence, fruits, and instrumentalities or things otherwise criminally possessed, derived, that are evidence of, or which have been intended for use as, the means of committing violations of Title 21, United States Code, Sections 846 and 841 (a) (conspiracy to possess with the intent to distribute controlled substance and attempts to do so) and to violations of Title 18, United States Code, Sections 922(g), 924(c) and 924(j); that involve members of the JORDAN DTO and/or their identified and unidentified co-conspirators, to include information or data stored electronically, only relating to the subject offenses if it is able to be determined at the time of seizure, including dialed-call telephone numbers; received-call telephone numbers; missed-call telephone numbers; names, telephone numbers. addresses and other data located in the address books or contacts databases; photographs; voicemails; emails and text messages stored, and/or removable SIM cards, and/or removable data cards, and data stored, audio/video files} including but not limited to the following:

- a. lists of customers and related identifying information;
- b. types, amounts and prices of drugs trafficked as well as dates, places, and amounts of specific transactions:
- c. any information related to sources of drugs (including names. addresses. telephone numbers, or any other identifying information);
- d. any information recording Anthony JORDAN or any identified and unidentified co-conspirator's schedules or travel to include any GPS data saved or stored on the devices to be searched:
- e. all bank records, checks, money orders, credit card bills, account

information, and other financial records;

- f. images or video regarding the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions;
- g. Images or video regarding the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions;
- h. Images or video regarding the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions;

2. Evidence: of user attribution showing who used or owned the **subject electronic device** to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet to communicate via mail, social media websites, or other electronic means, regarding customer purchases, shipments, financial transactions, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as Hash memory or other media that can store data) and any photographic form.

5. All data files, including but not limited to, records and graphic representations, containing matter pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.

6. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including but not limited to, JPG, GJF, TIF, AVI and MPEG) containing matter pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.

7. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the trafficking of controlled substances and controlled substance analogs through interstate or foreign commerce, including by United States mail or by computer, visual depictions, and records pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.

8. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related

financial transactions.

9. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.

10. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.

11. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture, distribution, or possession of controlled substances, possession of firearms in furtherance of the distribution of controlled substances, or any related financial transactions.